

# Public Key Infrastructure

Official  
Forms



Contracts



State  
Filing



Tax Return



Architectual  
Drawing



School  
Transcripts



*The Basis for E-Government  
In the Digital Kansas Future*

## Overview

The signing of the Uniform Electronic Transactions Act by the Kansas 2000 legislature laid the groundwork for Kansas to retain its position as one of the leading states providing efficient government through technology.

To turn legislation into reality, it is necessary to provide the infrastructure needed to achieve this environment. The essential element of this new environment is called Public Key Infrastructure (PKI).

PKI provides the means to enable an electronic transaction environment that does not ultimately require paper to finalize transactions. It provides the needed security and integrity to data and documents that are used in electronic transactions. It is also used to “digitally sign” electronic documents to satisfy requirements for transaction integrity and non-repudiation.

This brief pamphlet will begin to explain:

### **What is a digital signature**

- Why it is needed
- How it works
- What is needed to make it available

### **Why PKI is needed to provide secure transactions and digital signature**

- Description of Asymmetric Cryptography
- What are the components of PKI
  - Certificate Authority (CA)
  - Registration Authority (RA)
  - Key Repository
  - Certificate Practice Statement (CPS)
  - Certificate Policy (CP)

### **How this environment will be managed in Kansas**

- The role of:
  - Office of Secretary of State
  - Information Network of Kansas
  - Information Technology Executive Council

## What is a digital signature

A digital signature is not a digital picture of your signature. It is a method of linking your exclusive identity to an electronic document or transaction to accomplish what your written signature accomplishes in a paper document. According to the American Bar Association, a signature accomplishes several functions including but not limited to evidence, ceremony and approval of a writing.

A digital signature can be used to provide both signer and document authentication. Signer authentication is the ability to identify the person who digitally signed the document. Document authentication ensures that the document or transaction cannot be altered as a result of the digital signatures invocation.

### Why It Is Needed

The use of networked personal computers (PC's) in enterprise environments and on the Internet is rapidly approaching the point where they are considered mass media and a means to conduct a variety of online transactions

While the use of PC's and the software used on them has proliferated, an environment has evolved in which documents can be created, distributed, used and retained completely in digital form. When they are intended to support a business or legal transaction, some of these documents may require a signature as an endorsement, or authentication to be considered "official" or "authorized."

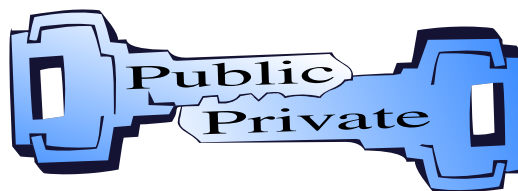
Until now, when a signature was either desired or required, such documents had to be converted to a paper in order to carry it. This simple act thus creates a variety of problems that frustrate both the flexibility and velocity of the transaction environment. It also creates retention management issues because the conversion to paper requires management of paper documents for their official life.

While the nature of the transaction these documents are meant to support has not changed, the environment in which the transaction is made is changing. To support the new environment

we must provide rules and practices that employ digital signature technology to achieve and surpass the functionality historically expected from paper based documents with ink signatures.

### Description of Asymmetric Cryptography

Cryptography is the science of creating and identifying code systems intended to scramble a readable message containing information (paper, email, etc.) so that the message cannot be understood by anyone other than an intended party. Asymmetric cryptography consists of a pair of codes (also called keys) used to scramble and de-scramble the message. The user has a private key to sign a message and a public key is available in a repository so the message can be verified by the receiver.



### How It Works

When you apply your digital signature to a document, it is used to create a hash value exclusive to the combination of your signature and the specific document. If the document were altered in any way, this hash value would not match and the document would be invalid and (in effect) lose the signature. Because it is computationally infeasible to derive one key from having the other, digital signature has great integrity. Consequently, it is more acceptable than other types of electronic signatures.

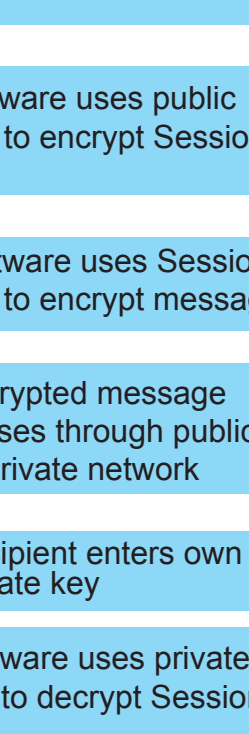
A digital signature looks like a random series of numbers and alphabetical characters. Each signature is unique because it uses the content of the electronic document to create the character string. An example of a digital signature is:

----- **BEGIN SIGNATURE** -----

idkflkmejsdaoiB441klklk08+kadlkdflioe993+1alkfdlasd4  
ksrlk41ksafij81kadflkl61ardifj+kdakljfl61adfldfjl+adfsdfddf+

----- **END SIGNATURE** -----





The diagram illustrates the asymmetric encryption process in two columns. The left column contains five light blue rectangular boxes with black text, and the right column contains five white rectangular boxes with black borders and text. Black arrows point downwards from each box in the right column to the next one below it.

**Left Column (Steps):**

- Sender enters message plus recipient's public key
- Software uses public key to encrypt Session key
- Software uses Session key to encrypt message
- Encrypted message passes through public or private network
- Recipient enters own private key
- Software uses private key to decrypt Session key
- Software uses Session key to decrypt message

**Right Column (Flow):**

- "Have a nice day"
- Public Key
- Session Key
- !1w6^8  
(5=I]:{k\$s#!
- Private Key
- Session Key
- "Have a nice day"

## What Is Needed To Make It Available

section. The operational component of PKI is largely the responsibility of the Certificate Authority acting under the direction of the State.

Training is also necessary so those users know when and how to apply signatures and what to do when they receive a signed document, email or other transaction in order to use it.

Finally, some level of marketing is needed to promote the use of digital signature as another way to conduct business between Kansas state agencies, citizens and the business community.

## Why PKI Is Needed To Provide Secure Transactions & Digital Signature

Many organizations, both public and private are interested in replacing paper-based systems with automated electronic systems. The reason for this is simple economics. It is much cheaper to process an electronic transaction with digital documents and signatures than with their paper counterparts.

Two factors have inhibited the increasing use of electronic documents and transactions. One has been the legal status of electronic documents. Simply put, there has been a cloud over the legitimacy of such documents. The other (related factor) has been the concern for the risk of forgery or manipulation of documents and data moving over unsecured networks. Both of these factors are rooted in a concern for the legitimacy and integrity of electronic documents and the security and privacy of the transactions for which they are used.

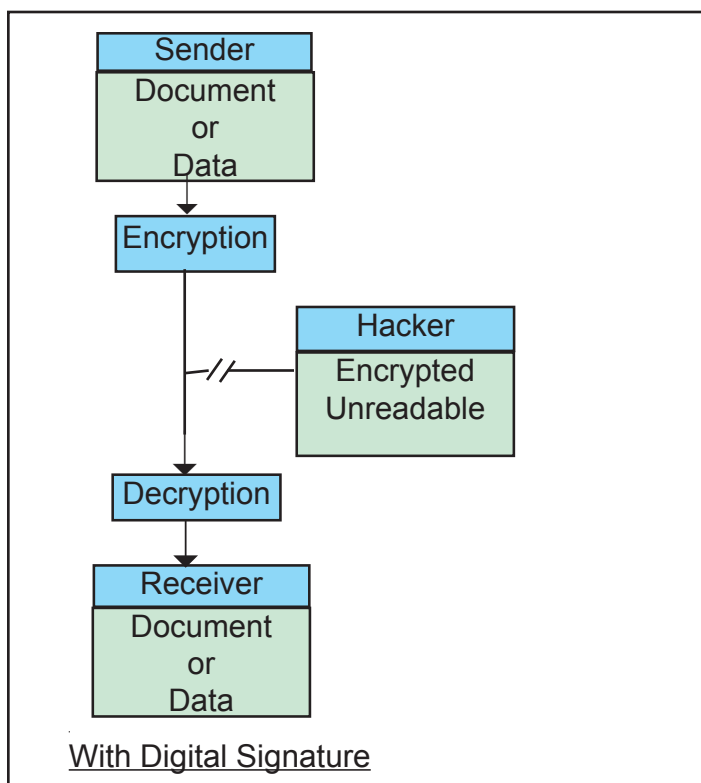
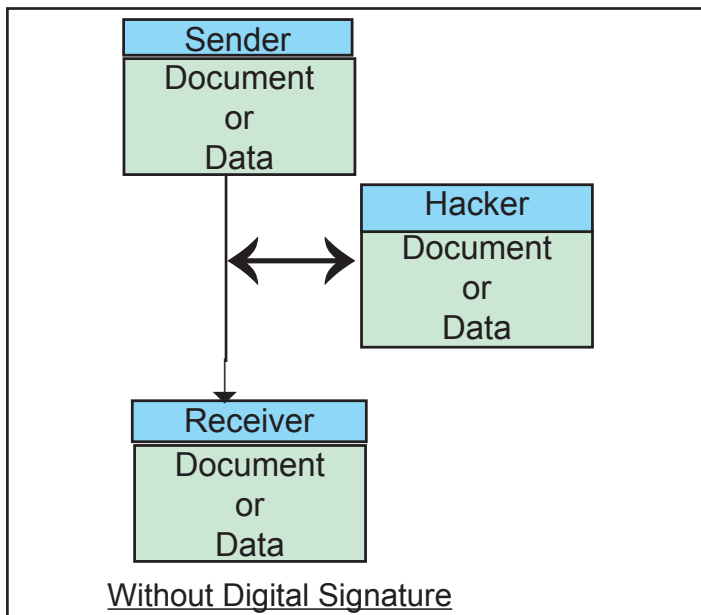
This has brought about the need for a reliable, cost-effective way to secure information in transit and to replace a handwritten signature with a



digital signature. The new Kansas law and similar federal legislation provide for the legitimacy of both electronic documents and signatures.

Thus, the legal status of electronic documents and signatures is resolved by addressing the issues of legitimacy, security and integrity. This is accomplished by insuring that information (document or data) in transit between two points is not intercepted and manipulated or otherwise tampered with.

The following figures illustrate this situation.



## What are the components of PKI

Just as highways, bridges and roads along with policies, laws and planning comprise a motor vehicle transportation infrastructure, PKI is comprised of a variety of components to enable a safe and secure electronic information exchange infrastructure. Each element of this infrastructure plays a role in the direction, management and operation of all the necessary functions.

### Certificate Authority (CA)

A CA is any service provider that takes responsibility for the issuing and maintenance of key pairs also referred to as digital certificates. The most comprehensive services will provide the full range of activities associated with PKI. This includes the following:

**Secure Facility** A secured facility where the data systems are protected physically from outside threats and operationally from service disruption. A goal of 100 percent availability with achievement in the range of 99.999 percent is a typical requirement.

**Key Issuance** Basically, this means that the CA maintains a listing of who was issued a key pair and a copy of each public key. At the wholesale level this means that they simply provide the keys to a Registration Authority (RA). The RA in turn is responsible for assigning a specific key set to a party. At the retail level it means that the CA would also make the assignment.

**Registration** This is also called “vetting” but by either name, it is the process associated with establishing some level of identity with the party to whom a key pair is associated.

**Repository** Housing the public keys of assigned key pairs is an ongoing task that involves maintaining keys and the associated identities behind them. This may also involve (in cooperation with affiliated RA's) renewal and revocation of keys and long term retention of expired keys. The repository service may be provided by an organization other than the CA.

**Key Access** The public keys of registered parties must be available from the CA along with the associated registration information. In effect, the CA acts as a clearinghouse by validating keys or making them available. This is sometimes referred to as “publishing” and may be part of the repository function when the CA functions have been distributed to multiple third parties.

## Registration Authority (RA)

An RA works in cooperation with a CA by providing the customer interface to an end user desiring a key assignment transaction for which the CA provides the technical infrastructure. The extent of the process can range from nothing more than establishing an email address to requiring an applicant appear in person with photo identification, birth certificate and other forms of proof including finger prints. The type of vetting required is called for in a formal structure called a Certificate Management Policy described below.

## Key Repository

This is a system that provides access to the “Public” keys or certificates that are used to sign and encrypt electronic messages and transactions.

The repository maintains expired and revoked keys for predetermined periods defined in the Certificate Management Policy.

## Certificate Practice Statement (CPS)

A document that establishes the operational practices that the CA will comply with in the delivery of their service to support the direction provided by the Certificate Policy.

## Certificate Policy (CP)

Having a CA in place and ready to issue certificates (key pairs) is not enough to complete the PKI

environment. There must be guidance to both CA and affiliated RA’s regarding their operations to insure a secure operation that can be relied on is maintained.

This comes in the form of a policy that dictates minimum standards for elements such as physical plant and data systems security, backup procedures, records retention and personnel qualification and management.

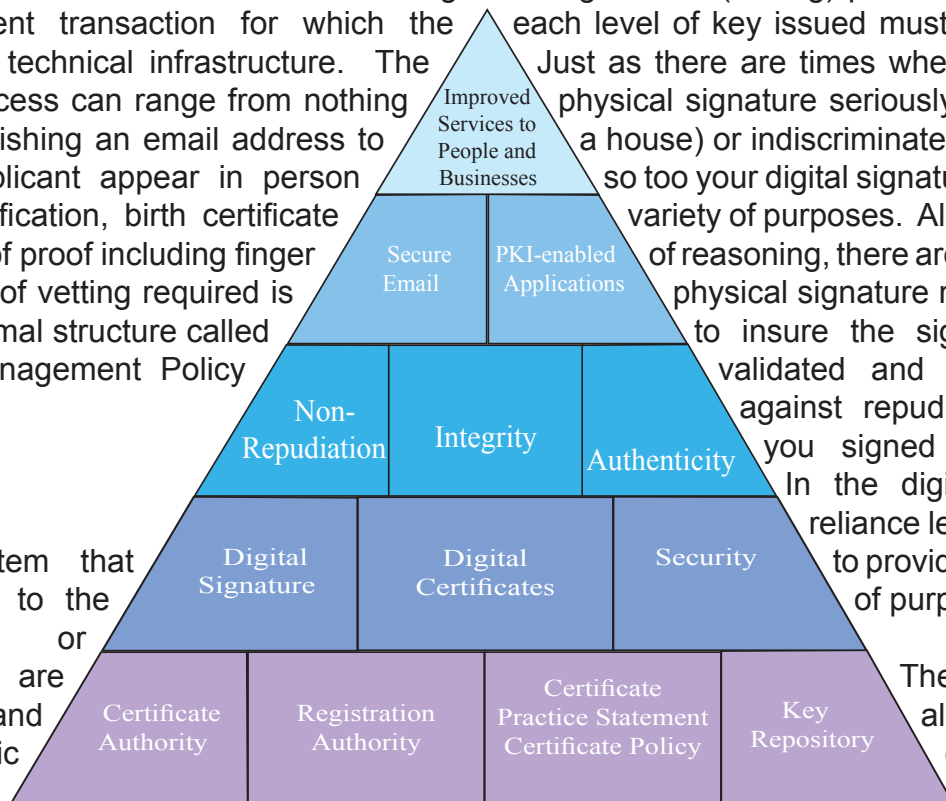
The type of keys that must be made available and the registration (vetting) process associated with each level of key issued must also be defined. Just as there are times when you apply your physical signature seriously (contract to buy a house) or indiscriminately (birthday card), so too your digital signature(s) may have a variety of purposes. Along the same line of reasoning, there are times when your physical signature must be notarized to insure the signer’s identity is validated and as a safeguard against repudiation (you deny you signed the document). In the digital world, these reliance levels are intended to provide the same range of purpose and security.

The certificate policy also provides direction to CA’s and RA’s regarding key (certificate) retention, expiry, revocation and renewal requirements.

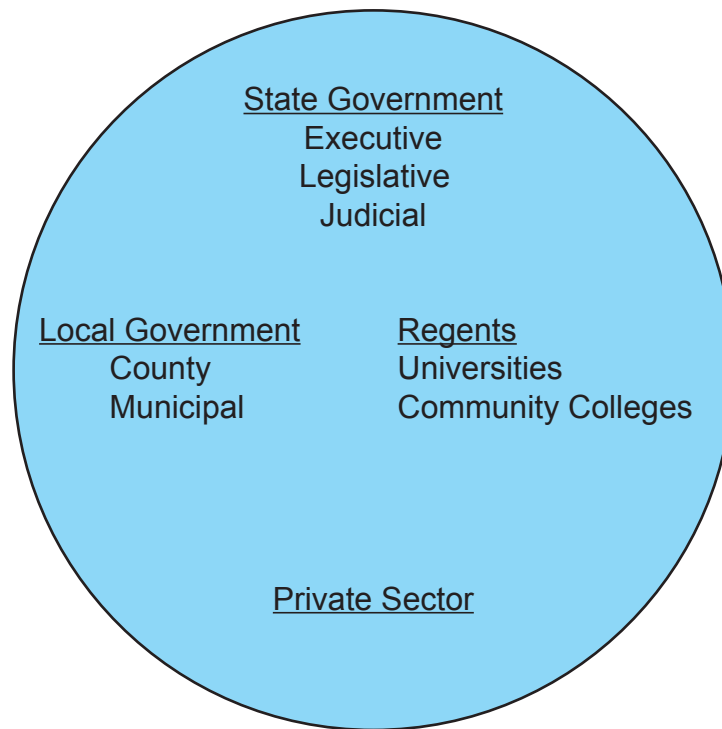
The certificate policy may be incorporated into a larger Certificate Practice Statement. This document speaks to the operational issues regarding such issues as security of the facility, systems availability, audibility and information protection and privacy.

## How This Environment Will Be Managed In Kansas

Security, integrity and non-repudiation of electronic documents, transactions and messages are some



## Information Technology Executive Council



of the goals of a fully developed PKI. To insure the infrastructure meets the needs of Kansas agencies and citizens, all branches of Kansas State government, in cooperation with private organizations, associations and academic institutions have participated in the development of the requirements for PKI.

The administration of this infrastructure is intended to meet the Syaye's requirements and continue active participation of these many organizations by distributing the roles and responsibilities for administration through the following organizations.

### Information Technology Executive Council

Each branch of Kansas government (Executive, Judicial, and Legislative) has a Chief Information Technology Officer that administers information technology policy and operations for their respective branch. Coordination by and between each government branch is accomplished at the Information Technology Executive Council (ITEC). ITEC was established by Kansas law (KSA 1998 Supp 75-7201 through 75-7212) to adopt Information Technology (IT) resource policies and procedures along with a technology architecture across all branches of state government. It must also provide direction and coordination for the state's IT resources, designate information

resource ownership and the lead agency for the implementation of new technologies and networks to be shared by multiple agencies in different branches of government.

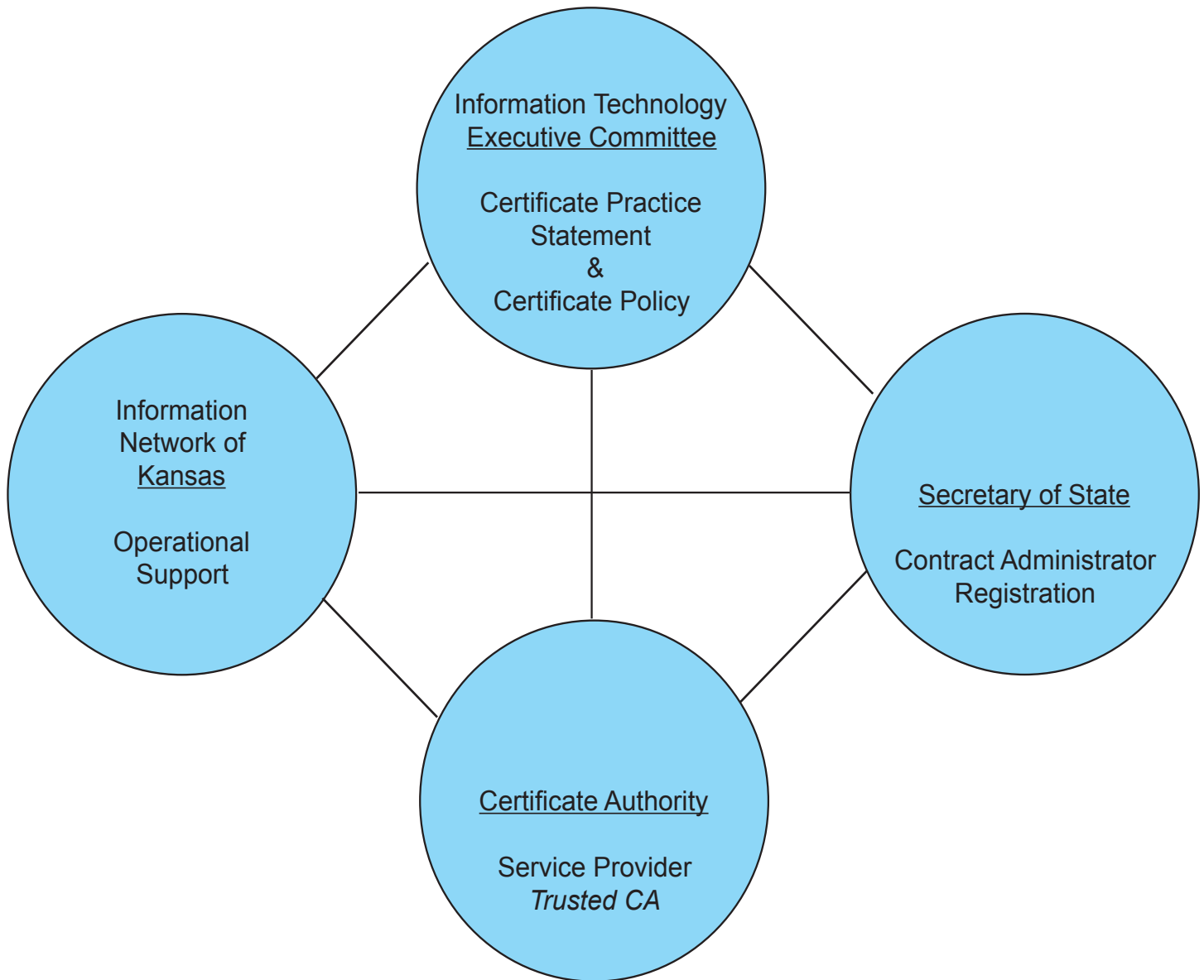
ITEC has a broad-based executive level committee that represents state and local government interests and the private sector. With such an expansive view of the needs of government and with the task to improve information technology for Kansas in general, it will be responsible for oversight of the official Kansas Certificate Policy.

### Office of Secretary of State

In order to provide services as a *Trusted Certificate Authority*, Kansas law requires the SOS to regulate the organization. The law also requires that the office establish rules and regulations to insure that *Trusted Certification Authorities* are qualified.

With the responsibility for registration of CA's and for establishing rules and regulations, the SOS will be responsible for any contract for Certificate Authority services in Kansas. This establishes a clear line of authority with regard to enforcement of the contract's terms and conditions and registration standing under the purview of the SOS.





### Information Network of Kansas

This organization was established by Kansas law (KSA 74-9303) for the purpose of providing equal electronic access to state, county, local and other public information to the people of Kansas. INK provides Kansas citizens equal access to governmental data via the Internet. As a public/private enterprise it is also charged with exploring ways and means of expanding the amount and kind of public information provided along improving citizen and business access to public information and providing add-on services. It is responsible for the states contract with the Kansas Information Consortium (KIC). KIC provides both free and subscription based Web services for Kansas state agencies to the using public. As part of this

agreement, INK receives payments from KIC. This fund is available to INK to further promote the adoption of relevant technologies in Kansas.

INK is a public and private sector enterprise. The Board of Directors is comprised of members from both sectors and its mission is to provide information and continually explore new ways to expand information along with the network to deliver it to benefit Kansas citizens and businesses.

INK has agreed to consider administering a support operation. It could also serve as an ombudsman Registration Authority for smaller agencies of Kansas government that do not have the capacity to provide this necessary function for their staff.